UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
CENTRAL DIVISION

IN THE MATTER OF THE SEARCH OF:

The content of the CD/DVD containing the search warrant production of Google Gmail Account, downloaded and currently in the possession of FBI Special Agent Benjamin Plante.

CASE NUMBER: 3:19-mj-77

SEARCH WARRANT

TO: SPECIAL AGENT BENJAMIN PLANTE AND ANY AUTHORIZED LAW ENFORCEMENT OFFICER OF THE UNITED STATES

An application by a federal law enforcement officer or an attorney for the government requests the search of the following property located in the District of South Dakota: The content of the CD/DVD containing the search warrant production of Google Gmail Account, downloaded and currently in the possession of FBI Special Agent Benjamin Plante.

The property to be searched, described above, is believed to conceal property which constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, concerning a violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

I find that the Application and Affidavit of Benjamin Plante, hereinafter incorporated by this reference, establish probable cause to search the account described in Attachment A and seize the items described in Attachment B.

cc: AUSA Miller
Agent
SKK

YOU ARE COMMANDED to execute this warrant on or before

November 22, 2019 (not to exceed 14 days)

☑ in the daytime – 6:00 a.m. to 10:00 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Mark A. Moreno, United States Magistrate Judge, or his designee.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized,

☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of

_____.

November 8, 2019 @ 3:31 p.m. Central Time at Pierre, South Dakota

Date and Time Issued

Mark A. Moreno

MARK A. MORENO
United States Magistrate Judge

RETURN		
Case no.: 3:19-mj-77	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated clerk of court.

_____

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The November 4, 2019, CD/DVD containing the content of the Gmail account associated with Dustin Joe Red Legs, currently in the possession of the Federal Bureau of Investigation, or any replacement CD/DVD downloaded from LERS if the current CD/DVD was not properly downloaded.

ATTACHMENT B

Particular Things to be Seized

Attachment A will be searched for the following information to the government for each user ID listed in Attachment A, for the time period of June 1, 2018, through the date of this order:

a. The contents of all emails associated with the account from June 1, 2018, to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. For the time period from June 1, 2018, to present: The contents of all communications and related transactional records for all Provider services used by the account subscriber/user (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination

addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

d. For the time period June 1, 2018, to present: The contents of all other data and related transactional records for all Provider services used by an account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including any information generated, modified, or stored by user(s) or Provider in connection with the account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

e. For the time period June 1, 2018, to present: All Provider records concerning the online search and browsing history associated with the account or its users (such as information collected through tracking cookies);

f. For the time period June 1, 2018, to present: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the account or by an account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

g. All records regarding identification of the account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

h. All device or user identifiers which have ever been linked to the account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers ("GUID"), mobile network information, telephone numbers, Media Access Control ("MAC") addresses, and International Mobile Equipment Identities ("IMEI");

i. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any Provider account (including both current and historical accounts) ever linked to the account by a common e-mail address (such as a common recovery e- mail address), or a common telephone number, means of payment (e.g., credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

j. For the time period June 1, 2018: All records of communications between Provider and any person regarding the account, including contacts with support services and records of actions taken;

k. All records, documents, files, and information relating to or stored on any of the following services: Android, Gmail, Google Books, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Docs, Google Groups, Google Hangouts, Google Maps, Google My Maps, Google Sites, Google URL Shortener, Google Voice, Location History, YouTube.

l. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

m. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252, those violations involving the user of the Provider account dustinjoeredlegs@gmail.com and occurring after June 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) All records, information, and communications, in whatever form, concerning violations of 18 U.S.C. §§ 2252;

(b) All records, information, and communications regarding Dustin Red Legs' calendar, schedule, meetings, phone calls, to-do lists, or travel;

(c) All bank records, check, credit card bills, account information, tax filings, and other financial documents;

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the user account, including records that help reveal the whereabouts of such person(s);

(g) The identity of the person(s) who communicated with the user account about matters relating to the 18 U.S.C. §§ 2252, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
CENTRAL DIVISION

IN THE MATTER OF THE SEARCH OF:	CASE NUMBER: 3:19-mj-77
The content of the CD/DVD containing the search warrant production of Google Gmail Account, downloaded and currently in the possession of FBI Special Agent Benjamin Plante.	**APPLICATION FOR SEARCH WARRANT**

I, Benjamin Plante, being first duly sworn upon oath, depose and state as follows:

I have reason to believe that within the CD/DVD previously provided by Google pursuant to a search warrant for the Gmail account "dustinjoeredlegs@gmail.com, here is now concealed certain property, namely: that described in the attached Affidavit in Support of Request for Search Warrant and Attachment A which I believe is property constituting evidence of the commission of a criminal offense, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, concerning a violations of 18 U.S.C. §§ 2251, 2252, and 2252A.

The facts to support a finding of probable cause are contained in my Affidavit filed herewith, and attached hereto and incorporated by this reference.

Respectfully Submitted,

Benjamin Plante
Special Agent, Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence on the 8th day of November 2019, at Pierre, South Dakota.

MARK A. MORENO
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The November 4, 2019, CD/DVD containing the content of the Gmail account associated with Dustin Joe Red Legs, currently in the possession of the Federal Bureau of Investigation, or any replacement CD/DVD downloaded from LERS if the current CD/DVD was not properly downloaded.

ATTACHMENT B

Particular Things to be Seized

Attachment A will be searched for the following information to the government for each user ID listed in Attachment A, for the time period of June 1, 2018, through the date of this order:

a. The contents of all emails associated with the account from June 1, 2018, to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. For the time period from June 1, 2018, to present: The contents of all communications and related transactional records for all Provider services used by the account subscriber/user (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination

addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

d. For the time period June 1, 2018, to present: The contents of all other data and related transactional records for all Provider services used by an account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including any information generated, modified, or stored by user(s) or Provider in connection with the account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

e. For the time period June 1, 2018, to present: All Provider records concerning the online search and browsing history associated with the account or its users (such as information collected through tracking cookies);

f. For the time period June 1, 2018, to present: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the account or by an account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

g. All records regarding identification of the account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

h. All device or user identifiers which have ever been linked to the account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers ("GUID"), mobile network information, telephone numbers, Media Access Control ("MAC") addresses, and International Mobile Equipment Identities ("IMEI");

i. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any Provider account (including both current and historical accounts) ever linked to the account by a common e-mail address (such as a common recovery e- mail address), or a common telephone number, means of payment (e.g., credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

j. For the time period June 1, 2018: All records of communications between Provider and any person regarding the account, including contacts with support services and records of actions taken;

k. All records, documents, files, and information relating to or stored on any of the following services: Android, Gmail, Google Books, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Docs, Google Groups, Google Hangouts, Google Maps, Google My Maps, Google Sites, Google URL Shortener, Google Voice, Location History, YouTube.

l. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

m. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252, those violations involving the user of the Provider account dustinjoeredlegs@gmail.com and occurring after June 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) All records, information, and communications, in whatever form, concerning violations of 18 U.S.C. §§ 2252;

(b) All records, information, and communications regarding Dustin Red Legs' calendar, schedule, meetings, phone calls, to-do lists, or travel;

(c) All bank records, check, credit card bills, account information, tax filings, and other financial documents;

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the user account, including records that help reveal the whereabouts of such person(s);

(g) The identity of the person(s) who communicated with the user account about matters relating to the 18 U.S.C. §§ 2252, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
CENTRAL DIVISION

IN THE MATTER OF THE SEARCH OF:	CASE NUMBER: 3:19-mj-77
The content of the CD/DVD containing the search warrant production of Google Gmail Account, downloaded and currently in the possession of FBI Special Agent Benjamin Plante.	**AFFIDAVIT IN SUPPORT OF REQUEST FOR SEARCH WARRANT**

STATE OF SOUTH DAKOTA)
)
COUNTY OF HUGHES)

I, Benjamin Plante, being first duly sworn upon oath, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent with the Federal Bureau of Investigation (FBI). I have been employed with the FBI since January 2018. From January to May 2018, I received training at the FBI academy, receiving training in all matters related to criminal investigations including but not limited to: evidence collection, search and arrest warrants, and criminal procedures. I currently am assigned to work violent crimes in Indian Country at the Pierre Resident Agency. As a Federal Agent, I am authorized to investigate violations of federal law of the United States and am a law enforcement officer with authority to execute warrants issued under the authority of the United States.

2. The facts set forth in this affidavit are based on the following: my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause for the requested warrant, it does not set forth all of my knowledge regarding this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the specified crimes have been committed by Dustin Joe Red Legs, who is – for the reasons set forth below – believed to be the user of the captioned account. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the specified crimes further described in Attachment B.

PROBABLE CAUSE

4. On September 25, 2018, Amy Pritzkau contacted Cheyenne River Sioux Tribe law enforcement (CRSTLE), indicating that she had found photographs of her daughter's vaginal area in her ex-boyfriend's email account. Cheyenne River Sioux Tribe Law Enforcement (CRSTLE) Detective Gordon Runs After Jr. and CRSTLE Officer Michael Condon initiated an investigation.

5. Pritzkau notified Detective Runs After, that on September 23, 2018, she provided her ex-boyfriend, Dustin Red Legs, with a place to stay at her residence located at 518 South Willow Street, Apartment 2, Eagle Butte, South Dakota.

6. Pritzkau advised Detective Runs After that she had found drugs in Red Legs' wallet in the past, so she searched his wallet for drugs on September 24, 2018. During this search, Pritzkau located a piece of paper with an email address (dustinjoeredlegs@gmail.com) and password on it.

7. Pritzkau told Detective Runs After that on September 25, 2018, she accessed the email account dustinjoeredlegs@gmail.com. In doing so, Pritzkau found two pictures of a vagina. After examining the pictures, Pritzkau indicated to Detective Runs After that she believed that the pictures were of her daughter Lola Big Eagle, date of birth March 13, 2008. Pritzkau believed she recognized clothing, bedding, and an injury located on her daughter's hand. Pritzkau then took screenshots of the photos located on this email account with her Samsung phone. The pictures were time stamped: September 24, 2018. Pritzkau told Detective Runs After that she remembered seeing Red Legs go into the room where the two oldest kids were sleeping a few times on September 24, 2018.

8. Detective Runs After contacted the Federal Bureau of Investigation to assist in this investigation. On September 25, 2018, your Affiant spoke with Pritzkau. She specified that the items in the pictures that helped her identify her daughter were the following: an injury on the index

finger of the female's right hand, a comforter, a zebra blanket, black shorts, and white underwear. The items led her to believe that the female was Lola Big Eagle. Big Eagle was present, and the injury was observed by your Affiant, and photographed by personnel at the Child Assessment Center in Pierre, South Dakota. Pritzkau then showed your Affiant the pictures located on her Samsung phone. Your Affiant was able to confirm that the material was pornographic and took photographs of these screenshots but before your Affiant was able to better inspect the images the phone's battery died. Upon reviewing the photographs taken by your Affiant, what appears to be a zebra blanket, black shorts, and white underwear were all visible in the photographs. The black shorts and white underwear were later collected from Pritzkau at her residence. Pritzkau then provided her consent to search the phone to your Affiant, and on October 3, 2018, Intelligence Analyst Justin Pederson, assigned to the NPSTDETF, completed a logical extraction of the Samsung phone. This extraction demonstrated that the previously mentioned email account dustinjoeredlegs@gmail.com was still open on her phone, but this email account was not accessed during this initial search.

9. Pritzkau also disclosed to your Affiant that after accessing these photos, Dustin Red Legs called her and asked her if she had a certain type of Samsung phone. Pritzkau believed that Red Legs received an email notification advising a mobile device had accessed his email account when she logged into the account with her Samsung phone. When Pritzkau told Red Legs that she did not know if she had that type of Samsung phone, Red

Legs replied, "oh shit" and hung up on her.

10. On September 25, 2018, at approximately between 10 p.m. and 11 p.m., Red Legs contacted Pritzkau on her Facebook account. Red Legs stated that he "fucked up", that he was going to shut his phone off forever, and that he wanted to kill himself.

11. On October 10, 2018, Intelligence Analyst Pederson executed the search warrant on Pritzkau's Samsung phone and completed two extractions on the device. The extractions revealed pictures of a child's vaginal area, a child who is believed to be Lola Big Eagle as the child had an injury on her right index finger and was wearing black shorts and white underwear. The results of these extractions revealed that the aforementioned pornographic images appeared to be in a Google Photos folder. Based on my training, knowledge, and experience, I have a reason to believe that this Google Photos folder was contained within the account's Google Drive.

12. A search warrant for the captioned account was obtained on August 12, 2019, but Google did not address the request before the search warrant had expired on August 26, 2019. No documents were received from Google by your Affiant.

13. On October 8, 2019, the United States Magistrate Judge Mark A. Moreno signed a second search warrant for the captioned account.

14. I, SA Plante, executed the Court's search warrant in this matter on October 17, 2019 by serving it on Google. Google did not provide the responsive materials within 14 days of the issuance of this Court's search

warrant. Google advised me on October 30, 2019 that the responsive materials were available for download via Google's Law Enforcement Request System (LERS). On November 4, 2019, I downloaded the materials to a CD/DVD. I have not reviewed the responsive materials and have not provided access to any other person to review them. It is my understanding that the United States seeks this additional warrant to review the responsive materials out of an abundance of caution to comply with the issue raised in the recent decision in *United States v. Nyah, 928 F.3d 694* (8th Cir. 2019).

15. Based on my training, knowledge, and experience as a law enforcement officer, I know that persons involved in the distribution of child pornography often keep records that include names and telephone numbers of customers, distributers, and other co-conspirators. Additionally, persons involved in the distribution of child pornography often have lists of persons who also distribute child pornography. Such lists may be maintained electronically on email accounts. I am also aware that individuals involved with the distribution of child pornography communicate through multiple medias, including telephone calls, text messages, emails, and Facebook messages.

16. Based upon my training and experience, I know that electronic files may be important to a criminal investigation in that they may be used to coordinate sales or purchases, to manage the records of a child pornography organization, or to store images or video that may be evidence of observation, possession, or distribution of child pornography. The warrant application in

this case requests permission to search the email account may be relevant to the possession or distribution of child pornography, because this account may contain files, text, images and/or video of pornographic activity involving a minor. I believe that in this case, the email account is a container for evidence and instrumentalities of the crime under investigation.

17. It is further reasonable to believe that pornographic images of a minor may be stored in the target e-mail account for the reasons set forth in paragraphs above.

18. Based upon the information above, I have probable cause to believe that Dustin Joe Red Legs used the captioned account to commit the specified crimes.

BACKGROUND CONCERNING EMAIL / ONLINE STORAGE

19. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

20. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the

registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, chat history, pictures (other than ones attached to emails), bookmarks and other files, including files associated with linked Google Documents applications, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. Services offered by Google include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as

Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

22. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the

account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling

the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications

relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. § 2703, by using the warrant to permit access to the CD/DVD I downloaded from the subpoena response previously provided by Google according to a search warrant. The file is particularly described in Attachment A. Upon receipt of the warrant, the government-authorized persons will review the contents of the file(s) on the CD/DVD to locate the items described in Attachment B.

27. As indicated above, I have not reviewed the content of the CD/DVD that the Google information was downloaded from LERS. If the current CD/DVD did not download properly, SA Plante will make a replacement CD/DVD downloaded from LERS.

CONCLUSION

28. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that in the download of the CD/DVD I downloaded from the subpoena response previously provided by Google in compliance with a previous warrant, there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google account, listed in Attachment A will contain evidence of the

crimes of 18 U.S.C. §§ 2251, 2252, and 2252A, which items are more specifically described in Attachment B. There is probable cause to believe that the likely user of the Google account was involved in or received evidence of the violations of the aforementioned statutes in the District of South Dakota and elsewhere. Therefore, there is probable cause to search the download of the CD/DVD, which contains the content of the Google/Gmail account associated with "dustinjoeredlegs@gmail.com".

29. Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully Submitted,

Benjamin Plante, Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence on the 8th day of November, 2019, at Pierre, South Dakota.

MARK A. MORENO
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The November 4, 2019, CD/DVD containing the content of the Gmail account associated with Dustin Joe Red Legs, currently in the possession of the Federal Bureau of Investigation, or any replacement CD/DVD downloaded from LERS if the current CD/DVD was not properly downloaded.

ATTACHMENT B

Particular Things to be Seized

Attachment A will be searched for the following information to the government for each user ID listed in Attachment A; for the time period of June 1, 2018, through the date of this order:

a. The contents of all emails associated with the account from June 1, 2018, to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. For the time period from June 1, 2018, to present: The contents of all communications and related transactional records for all Provider services used by the account subscriber/user (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination

addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

d. For the time period June 1, 2018, to present: The contents of all other data and related transactional records for all Provider services used by an account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services (for example, electronic communication services such as Google Voice, Hangouts, Google Groups, Google Photos, and YouTube; web browsing and search tools such as Google Search, Web History, and Google Chrome; online productivity tools such as Google Calendar, Google Contacts, Google Docs, Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); and online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries)), including any information generated, modified, or stored by user(s) or Provider in connection with the account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

e. For the time period June 1, 2018, to present: All Provider records concerning the online search and browsing history associated with the account or its users (such as information collected through tracking cookies);

f. For the time period June 1, 2018, to present: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the account or by an account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

g. All records regarding identification of the account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

h. All device or user identifiers which have ever been linked to the account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers ("GUID"), mobile network information, telephone numbers, Media Access Control ("MAC") addresses, and International Mobile Equipment Identities ("IMEI");

i. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any Provider account (including both current and historical accounts) ever linked to the account by a common e-mail address (such as a common recovery e- mail address), or a common telephone number, means of payment (e.g., credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

j. For the time period June 1, 2018: All records of communications between Provider and any person regarding the account, including contacts with support services and records of actions taken;

k. All records, documents, files, and information relating to or stored on any of the following services: Android, Gmail, Google Books, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Docs, Google Groups, Google Hangouts, Google Maps, Google My Maps, Google Sites, Google URL Shortener, Google Voice, Location History, YouTube.

l. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

m. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252, those violations involving the user of the Provider account dustinjoeredlegs@gmail.com and occurring after June 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) All records, information, and communications, in whatever form, concerning violations of 18 U.S.C. §§ 2252;

(b) All records, information, and communications regarding Dustin Red Legs' calendar, schedule, meetings, phone calls, to-do lists, or travel;

(c) All bank records, check, credit card bills, account information, tax filings, and other financial documents;

(d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the user account, including records that help reveal the whereabouts of such person(s);

(g) The identity of the person(s) who communicated with the user account about matters relating to the 18 U.S.C. §§ 2252, including records that help reveal their whereabouts.